Published and Copyright (c) 1999 - 2014
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1607 02/14/14

~ Steve Jobs Time Capsule! ~ People Are Talking! ~ Microsoft's New CEO!
~ Tempest 2000 Remake TxK! ~ Child Named 'Facebook' ~ PS4 Tops Sales List!
~ Berners-Lee Views on Web ~ Sony: No More PC Sales ~ Fix Your Passwords!

~ N Korea OS, Likens OS X ~ ~ FCC on Net Neutrality

-* Why Bad Guys Want Your Email *-
-* Internet Explorer Suffers Major Hack *-
-* Feds Launch Some Cyber Security Guidelines *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Happy day of cupids! It's been a very long week here, with a couple of nasty storms hitting the area this week, and another one forecast for the weekend. I'm not ashamed to say it, but I'm tired of it all for this season - I give up!! So, while we rest up here in the Northeast, let's get right to this week's issue!

Until next time...

=~=~=~=

->In This Week's Gaming Section - PS4 Tops List As US Videogame Console Sales Climb!
""""""""""""""""""""""""""""""""" Tempest 2000 Remake TxK Blasts Its Way Onto PS Vita

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

PS4 Tops List As US Videogame Console Sales Climb

US videogame hardware sales surged in January, with Sony s new-generation PlayStation 4 consoles leading the charge, according to figures released on Thursday.

People spent $241 million on videogame hardware, predominately consoles, in January compared to $205 million in the same month a year earlier, when a fifth leap week gave figures a particular boost, according to industry tracker NPD Group. Sony s PS4 led overall hardware sales,

followed by Microsoft new-generation Xbox One consoles, NPD reported.

PS4 sales were nearly double that of Xbox One in the month, Sony said citing the NPD report.

Demand for PlayStation 4 remains incredibly strong, Sony PlayStation brand marketing senior VP Guy Longworth said in a release.

It s clear gamers are choosing PlayStation as the best place to play. Membership in the PlayStation Plus subscription service for games, films, and other digital entertainment has nearly doubled since the PS4 launched in November, according to Sony.

Meanwhile, videogame software sales sank about 40 percent in November to $224 million, down from $373 million in January of 2013.

The decline was due to a big drop in the number of new titles released for play, said NPD analyst Liam Callahan.

Activision s military shooter game Call of Duty: Ghosts was the best selling game on a top 10 list that included Assassin s Creed IV: Black Flag and Grand Theft Auto V .

Traditional format videogame sales overall for January were $664 million, down 21 percent from the prior January but nearly flat if the extra leap week is factored in, according to NPD.

When money spent on mobile games, rentals, digital downloads, subscriptions and social network play are added in, sales for January tallied $1.05 billion, NPD reported.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Tempest 2000 Remake TxK Blasts Its Way Onto PS Vita

TxK, Jeff Minter’s remake of the Atari Jaguar game Tempest 2000, will be available on PS Vita alongside the PlayStation Store update. In TxK, players travel down a corridor while shooting obstacles; special musical bonus stages, which players cannot fail, are scattered throughout TxK.

"We’ve tried to create something that is pure and beautiful in the same way as the old abstract vector-graphics arcade games, but vibrant and modern in aspect and effects as you play," Minter wrote on the PlayStation Blog. "You’ll blast your way through 100 levels and 3 different game modes to keep you challenged whether you want a long session or a quick 5 minutes of gaming on the go."

Minter’s TxK was originally due to launch last year. A lengthy gameplay video of TxK, available (see link below), should give you an idea of what to expect: an explosion of color set to a thumping techno soundtrack. And

perhaps a llama or two.

https://www.youtube.com/watch?v=Q2TTa0z2o0M

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Feds Launch Cyber Security Guidelines For US Infrastructure Providers

The White House on Wednesday released the first version of its cyber security framework for protecting critical infrastructure. Critics say these voluntary guidelines enshrine the status quo.

The White House on Wednesday released the first version of its cyber security framework for protecting critical infrastructure. It's a catalog of industry best-practices and standards that creates a voluntary template for companies to use in developing better security programs.

The Framework for Improving Critical Infrastructure Cybersecurity "enables organizations - regardless of size, degree of cybersecurity risk, or cybersecurity sophistication - to apply the principles and best-practices of risk management to improving the security and resilience of critical infrastructure," the White House said in a statement.

Although the document was hailed by administration officials as a "major turning point" in cybersecurity, it contains little that is revolutionary or even new. The National Institute of Standards and Technology, working with the Homeland Security Department and industry stakeholders, has compiled a set of known, publicly vetted standards that can be applied to identify, protect from, detect, respond to, and recover from risks.

The framework is technology-neutral and does not specify tools or applications to be used. Choices of technology are left to the user in addressing each category of risk management.

The framework is built on three basic components:

Core. A set of common activities that should be used in all programs, providing a high-level view of risk management.
Profiles. These help each organization align cybersecurity activities with its own business requirements, and to evaluate current risk management activities and prioritize improvements.
Tiers. Tiers allow users to evaluate cybersecurity implementations and manage risk. Four tiers describe the rigor of risk management and how closely it is aligned with business requirements.

The framework is one leg of a three-pronged program set out in a presidential executive order on protecting privately-owned critical infrastructure, issued one year ago in response to Congress's failure to

pass cybersecurity legislation. The second leg involves information sharing among companies and between the public and private sectors. The third leg attempts to address the protection of privacy and civil liberties.

Privacy was a difficult area for stakeholders to come to a consensus on during the five public workshops and multiple iterations of the document. Some protections are incorporated in instructions for using the framework, but privacy was identified as an area that needs to be better addressed in future versions.

Although it would be difficult today for any attack to cause widespread, long-lasting damage to the nation’s critical infrastructures, cyberattacks are becoming more effective. Demonstrated weaknesses in the IT systems that control and support the energy, transportation, financial services industries, and others leave them vulnerable to these attacks.

Although the framework is voluntary and will depend primarily on "enlightened self-interest" to drive its use, it is not entirely without teeth. Regulatory agencies are working to harmonize existing regulations with the document, and government procurement requirements are likely to include conformance to the framework for contractors and suppliers.

But one White House official said during a briefing, "The goal is not to expand regulation."

Other incentives for adoption are expected to include public recognition, cyber insurance and cost recovery programs, all of which can be implemented without legislation. Administration officials said they will ask Congress for additional authority as needed, for protections such as limitations on liability for companies adopting the framework. But given the slow pace of legislation in the current Congress the administration’s goal is to convince companies operating critical infrastructure that using the framework would be a good business decision.

Drafters said the framework creates a shared vocabulary for discussing and describing cybersecurity that can be used by a broad range of companies in different industries to create and evaluate risk-management programs. Gaps in programs can be identified and plans tailored to meet the specific needs for each user.

In an effort to support adoption of the framework by the private sector, the Department of Homeland Security is also launching a voluntary Critical Infrastructure Cyber Community program. According to DHS Secretary Jeh Johnson, the program will provide a "single point of access" to the department’s cybersecurity experts for anyone needing help or advice.

Although the program is just getting underway, one of its services, the Cyber Resilience Review, has already been widely used by industry. The review lets organizations assess their current programs and determine how well they are aligned with the practices and standards of the framework. More than 300 of the reviews have been carried out.

President Obama, in a prepared statement, called the framework a turning point, but added, "It’s clear that much more work needs to be done," a sentiment shared by the document’s supporters and detractors alike.

Bob Dix, VP of global government affairs and public policy for Juniper

Networks, called it "a laudable first step," but said "there is more that government and industry must do together to address basic cyber hygiene as well as the most sophisticated and persistent threats to critical infrastructure."

Because the framework is based on existing practices and standards, it has been criticized as enshrining the status quo rather than advancing cybersecurity. NIST officials said it is a living document that will be regularly updated.

A preliminary draft of the framework laid out areas for improvement to be addressed in future versions. These include authentication, automated information sharing, assessing compliance with standards, workforce development, big data analytics, international impacts, privacy standards, and supply chain management.

Why The Bad Guys Want Your Email

Your email just got broken into? Sorry, it s not personal. It s business.

That may not console you much when you realize that your email account was pwned through malware or deceit. But, really, the hackers who went after it probably had nothing against you personally. They were instead focused on potentially profitable uses of your email.

This is a point that can easily get lost in the coverage of nightmare hacking scenarios like the 2012 instance in which Wired writer Mat Honan had his Gmail and iCloud accounts hijacked, then saw his iPhone, iPad and MacBook remotely wiped, all so a teenage guy could have fun broadcasting inanities from his three-character Twitter handle @mat.

But, most of the time, crooks going after your email have nothing more ambitious in mind than using it to spam people about fraudulent offers or malicious downloads.

 For the most part, compromised webmail accounts are used to send spam (some of which may contain links to malware), writes Johannes Ullrich, chief research officer at the SANS Institute.

In a subsequent conversation, he said that not only has the use of hacked email addresses for spam stayed pretty much constant, but in some ways such addresses have become more valuable. How so? Stronger authentication systems deployed by major mail services have made it harder to send a spoofed message one that looks like it s from a legitimate address when it isn t. So, since email impersonation is harder, the bad guys need to take over accounts to send messages that look real.

What else can a hacker do with a hijacked account? McAfee public-sector chief technical officer Scott Montgomery sketched out one easy possibility: Let s say I compromise your Yahoo mail, your Google mail, whatever what is the likelihood that you have reused that same password at multiple locations?

That s right. Stealing one password can open up access to a multitude of a user s accounts. So take this opportunity to redo yours; for the most security, use a service like LastPass, 1Password or Dashlane to generate and store random passwords for you.

But even if a victim was smart enough to use different passwords for anything of serious value, it won t matter if an attacker can reset them online with the only needed confirmation being a click on an email sent to an inbox that the attacker already controls.

Or, as Brian Krebs reported last March, the attacker can skip even that minimal step by asking the bank nicely via email for help completing a wire transfer.

Ullrich said SANS hasn t seen too many instances of this, thanks mainly to the fact that it s more profitable to confine that particular scam to cases where they know that this person deals with large amounts of money.

In one particularly ambitious attack SANS is investigating, the scammer steps into existing business correspondence to try to fool a customer into sending money to the wrong place. It appears to happen quite a bit with real estate, Ullrich observed.

Montgomery suggested one last, still uglier use for a hijacked email: Instead of just spamming friends with some bogus offer, they try to get them to click and install ransomware that then locks them out of their own files unless they pay off the scammer.

A site password plus an email address that itself is secured with only a password shouldn t open the door to moving money around. But while most Web-mail services now offer two-step verification yes, you should turn it on only a handful of name-brand banks and other financial institutions also do.

I don t think you can legislate a requirement for two-step verification, but having to reimburse enough customers for losses ought to have an educational effect on banks that haven t let customers lock their accounts with more than a username and password.

That doesn t mean the folks in Washington have nothing at all to do on this front. Beyond the absence of a national law requiring companies to notify you if they lose your data, the primary law aimed at networked crime the Computer Fraud and Abuse Act needs a rewrite of its own.

That s not because it s too tolerant of hacking attempts; it s because it now defines them so broadly that it can be used to target legitimate security research. In an upcoming column, I ll explain why the CFAA has become many techies least favorite law.

Internet Explorer Suffers Major Hacking Attack

A previously unknown flaw in a recent version of Microsoft Corp. s Internet Explorer web browser is being used to attack Internet users, including some visitors to a major site for U.S. military veterans, researchers said Thursday.

Security firm FireEye Inc. discovered the attacks against IE 10 this week, saying that hundreds or thousands of machines have been infected. It said the culprits broke into the website of U.S. Veterans of Foreign Wars and inserted a link that redirected visitors to a malicious web

page that contained the infectious code in Adobe Systems Inc. s Flash software.

FireEye researcher Darien Kindlund said the attackers were probably seeking information from the machines of former and current military personnel and that the campaign shared some infrastructure and techniques previously attributed to groups in mainland China.

He said planting backdoors on the machines of VFW members and site visitors to collect military intelligence was a possible goal.

A VFW spokeswoman didn t immediately respond to requests for comment.

A Microsoft spokesman said the company was aware of the targeted attacks and was investigating. We will take action to help protect customers, spokesman Scott Whiteaker said.

The latest version of the browser is IE 11, which is unaffected, and a Microsoft security tool called the Enhanced Mitigation Experience Toolkit also protects users who have installed that.

Previously unknown flaws in popular software are a key weapon for hackers and are sold by the researchers who discover them for $50,000 or more, brokers say.

They are most often bought by defense contractors and intelligence agencies in multiple countries, but some of the best-funded criminal groups buy them as well.

FCC Head Says He’ll Preserve Open Internet

The Federal Communications Commission is plotting to restore the net neutrality rules that were invalidated by an appellate court last month, Chairman Tom Wheeler said this week.

In a speech delivered on Monday at the University of Colorado Law School, Wheeler said he intends to preserve a free and open Internet. The FCC head has yet to provide specifics. Instead, he said only that he intends soon to outline how he wants to proceed.

In January, the D.C. Circuit Court of Appeals gutted the FCC’s net neutrality rules, which prohibited broadband providers from blocking lawful content or apps. The court ruled that the FCC couldn’t impose common carrier regulations on broadband providers, given that the agency classified broadband as an information service in 2002.

Neutrality advocates now say the FCC must first reclassify broadband as a telecommunication service if the agency wants to impose neutrality rules that will stand up in court. That way, broadband providers will be subject to the same common carrier rules that require telephone companies to put through all calls.

If Wheeler intends to take that route, he’s keeping it a secret - to the dismay of advocates. On Friday, the group Free Press made another push to convince Wheeler to reclassify broadband as a telecommunications service.

If the Commission fails to restore common carriage to our nation s

central communications network, we are ensuring that future generations of Americans will not be able to send the information of their choosing, between points of their choosing, without undue discrimination, the group says in a letter to Wheeler. Is the Commission really prepared to tell our children that if they want to act like their parents and grandparents and make a voice call using a landline or wireless phone, they know that call will connect and won t be of inferior quality, and they won t be price gouged for it; but if they instead choose to communicate through their natural medium of data, they get no legal protections against undue discrimination?

Free Press isn't the only one urging the FCC to move on neutrality. Five Democratic senators warned Wheeler this week that the recent appellate court ruling gutting neutrality rules threatens the freedom of innovators to compete on an open, neutral platform.

We urge you to quickly adopt enforceable rules to prevent the blocking and discrimination of Internet traffic, the lawmakers say in a letter to Wheeler. Without such rules in place, Internet service providers are prone to act as gatekeepers of the Internet, controlling access by blocking or throttling certain content and thereby limiting the opportunities for innovation, speech and commerce.

The letter was signed by Sens. Al Franken (D-Minn.), Ron Wyden (D-Ore.), Jeff Merkley (D-Ore.), Ed Markey (D-Mass.), and Richard Blumenthal (D-Conn.).

Tim Berners-Lee: We Need To Re-decentralise The Web

Twenty-five years on from the web's inception, its creator has urged the public to re-engage with its original design: a decentralised internet that at its very core, remains open to all.

Speaking with Wired editor David Rowan at an event launching the magazine's March issue, Tim Berners-Lee said that although part of this is about keeping an eye on for-profit internet monopolies such as search engines and social networks, the greatest danger is the emergence of a balkanised web.

"I want a web that's open, works internationally, works as well as possible and is not nation-based," Berners-Lee told the audience, which included Martha Lane Fox, Jake Davis (AKA Topiary) and Lily Cole. He suggested one example to the contrary: "What I don't want is a web where the Brazilian government has every social network's data stored on servers on Brazilian soil. That would make it so difficult to set one up."

It's the role of governments, startups and journalists to keep that conversation at the fore, he added, because the pace of change is not slowing - it's going faster than ever before. For his part Berners-Lee drives the issue through his work at the Open Data Institute, World Wide Web Consortium and World Wide Web Foundation, but also as an MIT professor whose students are "building new architectures for the web where it's decentralised". On the issue of monopolies, Berners-Lee did say it's concerning to be "reliant on big companies, and one big server", something that stalls innovation, but that competition has historically resolved these issues and will continue to do so.

"It’s important to have the geek community as a whole think about its responsibility and what it can do"

Sir Tim Berners-Lee

The kind of balkanised web he spoke about, as typified by Brazil’s home-soil servers argument or Iran’s emerging intranet, is partially being driven by revelations of NSA and GCHQ mass surveillance. The distrust that it has brewed, from a political level right down to the threat of self-censorship among ordinary citizens, threatens an open web and is, said Berners-Lee, a greater threat than censorship. Knowing the NSA may be breaking commercial encryption services could result in the emergence of more networks like China’s Great Firewall, to "protect" citizens. This is why we need a bit of anti-establishment push back, alluded to by Berners-Lee.

He reiterated the need to protect whistleblowers like Edward Snowden that leak information only in extreme circumstances "because they have this role in society". But more than this, he noted the need for hackers.

"It’s a really important culture, it’s important to have the geek community as a whole think about its responsibility and what it can do. We need various alternative voices pushing back on conventional government sometimes."

In the midst of so much political and social disruption, the man who changed the course of communication, education, activism and so much more, and in so many ways, remains dedicated to fighting for a web founded in freedom and openness. But when asked what he would have done differently, the answer was easy. "I would have got rid of the slash slash after the colon. You don’t really need it. It just seemed like a good idea at the time."

Microsoft s New CEO: We Have the Best Platform to Change the World

On Tuesday morning, Microsoft unveiled its new CEO: Satya Nadella, its former executive vice president of cloud and enterprise. Though Nadella has spent 22 years at Microsoft, there are not many outside of Microsoft who are familiar with the new CEO.

So consider the video - (https://www.yahoo.com/tech/meet-microsofts-new-ceo-satya-nadella-75089257289.html) as well as our own primer on Nadella an introduction. With its announcement, Microsoft included Nadella s first interview as CEO of Microsoft, a video conversation with fellow Microsoft executive Steve Clayton. Not surprisingly, Clayton doesn t have many hard-hitting questions for his new boss. The video plays more as an attempt to humanize a man we know little about while assuring the viewer that, in spite of the perception of Nadella as a company man, he may be looking to rock the boat a bit.

Asked what he actually plans on doing in the new role, Nadella suggests that he s going to come out swinging: First thing I want to do and focus on is ruthlessly remove any obstacles that allow us to innovate every individual in our organization to innovate and then focus all of that innovation on things that Microsoft can uniquely do.

As to what it is that Microsoft can actually do, the new CEO s answer unsurprisingly focused on mobile and cloud solutions the latter his own area of expertise, and the former an area in which the company has lost a fair amount of footing in recent years, with a late entry into smartphones and the continued struggles of its Windows Phone operating system against Apple s iPhone and Google s Android phones.

 It s a mobile-first, cloud-first world, Nadella explains in the video. Everything is becoming digital and software-driven. And so I think of the opportunities being unbounded. We need to be able to pick the unique contribution that we want to bring. And that s where our heritage of having been the productivity company to now being the do-more company, where we get ever individual and every organization to get more out of every moment of their life, is what we want to get focused on.

Actually, Nadella uses the phrase the do-more company multiple times in the video, suggesting that it s a motto Microsoft has been using internally to describe itself.

The new CEO is certainly right when he suggests that this is a software-powered world. Nadella doesn t have a lot to say yet with regard to the company s recent inability to take advantage of that fact, but no one reasonably expected him to take his predecessor Steve Ballmer down a peg in his entrance interview particularly in light of the fact that reports pointed to a close working relationship between Nadella and Ballmer.

In the video, Nadella is, not surprisingly, bullish about MS s prospects, saying, We have the talent, the resources and perseverance like no one else has. And then you take that and combine it with the fact that the world going forward is more of a software-powered world, delivered in devices and services I think we have the best platform to change the world.

That might be true. But now the real hard work will begin.

Sony Will No Longer Sell Personal Computers

Sony, like the rest of the industry, has seen its PC sales tumble as people rely more and more on the tiny computers they carry around in their pockets. On Tuesday that reality led to a huge shift in Sony s business: The company will be selling off its Vaio PC line. Sony confirmed that it has found a buyer for its branded Vaio computers in Japan Industrial Partners, a Japanese investment group.

The plan to exit the PC market has been in the works for a while, according to the company. Back in 2012, Sony began aggressively employing a restructuring that designated imaging (cameras), gaming (PlayStation) and mobile (phones/tablets) as the foundation of its electronics business. The move left two major categories out on the fringes: TVs and PCs.

While the company notes that the TV business won t become profitable by the time the fiscal year ends next month, it happily noted that it has managed to significantly enhance its operational structure and product competitiveness. Indeed, any reporter who has attended a Sony event in

the past year can tell you that TV namely 4K is still a major focus for the company.

Sony will be spinning its TV division off as its own business. The Vaio line, on the other hand, will be sold, after 17 years within Sony. There aren t any specific numbers on the proposed deal, but Sony noted that between 250 and 300 employees will likely be hired by Vaio s new owners. Others will be transferred to different divisions in Sony, and the rest will be offered early retirement plans.

The Vaio sale comes amid news that the company will be shedding 5,000 jobs or around 3 percent of its full staff.

Here in the States, at least, the Vaio never really became the major player Sony hoped it would. Still, the company won fans among tech reviewers, and some PC shoppers, for its innovative and lightweight laptop. A recent story even noted that Apple s late founder Steve Jobs counted himself a fan, once suggesting that Sony become the sole third-party manufacturer building devices to run OS X, Apple s desktop operating system.

While Sony never achieved the sales of some of the top PC makers, it s hard not to see such a sale as a sign of the times for the computing industry. It would be going too far to suggest that this marks the beginning of the end for laptops and the like, but it certainly doesn t bode well when a company as large and innovative as Sony sees the writing on the wall.

North Korea’s Home-grown OS Looks A Lot Like Apple’s OS X

If imitation is the sincerest form of flattery, might the folks in Cupertino be pleased when they see the latest version of North Korea s home-grown operating system?

Version 3.0 of Red Star Linux presents users with a radical refresh of its desktop design, one that closely resembles Mac OS X. The new look replaces the Windows 7-like desktop that was used in version 2.0 of the software.

The Korea Computer Center (KCC), a major software development center in Pyongyang, began developing Red Star about a decade ago. Version 2 is 3 years old and version 3 appears to have been released in the middle of last year.
140130 redstar background

The world has gotten its first look at version 3 thanks to Will Scott, a computer scientist who recently spent a semester teaching at the Pyongyang University of Science and Technology (PUST). The school is North Korea s first foreign-funded university and many of the lecturers come from overseas.

Scott said he bought the operating system at a KCC dealer in the capital city and the screenshots he provided were of the basic version 3 software without any modifications.

While most North Koreans are restricted from accessing the Internet, many can get access to a nationwide intranet through universities and public

libraries. The intranet offers websites for domestic institutions and is heavily skewed towards offering information, educational materials such as PDF versions of books and scientific papers, and government propaganda.

Red Star Linux includes a web browser based on Mozilla that has been re-branded Naenara, or My country.

It also includes a copy of Wine, a Linux application that provides an environment under which Windows software can be run.

’Steve Jobs Time Capsule’ Discovered

In 1983, Steve Jobs, the late co-founder and CEO of Apple Inc., gave a speech to a small audience at the International Design Conference in Aspen, Colo. The Macintosh computer hadn t been introduced yet, but Jobs was already predicting the rise of the personal computer, wireless networking, an easy-to-use and portable computer, and the ability to sell software without a brick-and-mortar store.

The speech has since become a part of the Steve Jobs legend as evidence of how visionary he was. At the end, Jobs added the Apple Lisa mouse he used during the talk to a time capsule full of objects donated by conference attendees.

Apple Lisa Mouse The "Steve Jobs Times Capsule" containing the Lisa mouse Jobs used during a legendary speech in Colorado, was found after 30 years.

The inclusion of the Lisa mouse gave the capsule the name of The Steve Job Time Capsule, and after a failed attempt to unearth it in 2000, the priceless piece of tech history was thought to be lost forever.

Until September, when a crew working National Geographic Channel s Diggers discovered and dug up the Steve Jobs Time Capsule. Protected in a plastic bag among a six-pack of beer, a Moody Blues cassette and a Rubik s cube, the crew found Jobs personal Lisa mouse.

The discovery will kick of the latest season off Diggers, which premieres on the National Geographic Channel on Feb 25.

Weekend Project: Fix Your Passwords

By now you know that the only thing keeping your online accounts safe is the thin wall known as the password. On most sites, if your password is stolen, your account is wide open. Whoever gets your password can impersonate you, steal money from you and erase your valuable digital assets, like your photos.

It matters what you choose as a password. If bad guys are attacking a site you use, or have gotten a list of encrypted passwords from a site, then the longer and more random the password, the harder it will be to discover. So you want your passwords to be as strong as possible. What s a strong password? Not password, or 123456, or anything else on the

list of dumbest passwords people use; those are the ones hackers will try on your accounts first.

You also need your passwords to be different on each site. That way, if a password to one site is stolen, the damage will be contained. The last thing you want is for one site you use to get hacked, exposing your data to criminals not just there, but everywhere.

The problem, of course, is that while everyone knows what a strong password looks like a long string of random letters, numbers and symbols nobody wants to come up with strong passwords, and no normal person could possibly memorize dozens of strong, random passwords for the sites they use.

But doing just that is the only safe thing to do. Anything less using weak passwords, or the same password in multiple places is asking for trouble.

So, to summarize: Only absurd, un-memorizable passwords are safe. You can t write them down. And you need a different password on each site. No wonder nobody practices good password hygiene. It s just not possible.

At least, not without help. There is a solution, one that we at Yahoo Tech cannot recommend highly enough: Use a password manager. That s a program that memorizes all your complicated passwords for you.

So let s get your passwords into shape, shall we? Welcome to the weekend project: fixing your passwords (with a password manager).

Step 1: Get started with a password manager.

There are several competing password managers. These apps will create good passwords, remember them for you, store them safely, synchronize them across your computers and mobile devices, and even enter passwords into your login forms so you don t have to type them. If you need good passwords and you do then using a password manager is the best way to fly.

Now, one warning: All the passwords you store in a password manager are protected by a password. So you have to be sure that the password you choose to protect your vault is a good one. But at least it will be the only one you need to remember. And remembering one long password once is a lot easier than remembering a hundred of them. Or worse, storing them someplace insecure.

There are alternatives to these password managers. In particular, if you use nothing but Apple products, and only Apple s Safari browser, then Apple s iCloud Keychain, a part of the latest operating systems for Macs, iPhones and iPads, can do a lot of what a password manager does.

And then there s the trick that a lot of people use to keep dozens or hundreds of passwords in their heads: They use a cipher for generating their own unique passwords for each account, by combining a strong password with a method of substituting the name of the site they re visiting into it. For example, let s say my core password is Fi33ykit10s!, and my cipher is to use the second letter of a site I m visiting at the beginning of the password, and the number of characters in it as the second-to-last character. So my password for Yahoo would be aFi33ykit10s5!. No dictionary lookup will find that.

The cipher method works until you come across a site where the password rules obviate your system, like not allowing special characters, or a minimum or maximum password length that doesn t work for your password.

So use a password manager. Here are some of the best ones out there:

1Password: My preferred system. Nice interface. Remembers credit-card numbers. Auto-enters passwords in websites. Synchronizes a highly encrypted database of your passwords over either iCloud or Dropbox (or some other homebrew system, if you want). But it s expensive: $49.99 for the Mac or Windows version, plus $17.99 for the iPhone version. Bundles and deals are sometimes available.

Password managers like 1Password (shown) will remember all your passwords and automatically put them into Web login forms.

LastPass: Does pretty much everything 1Password does, but it s not as pretty. Has finer-grained security controls, including two-factor authentication (so even if someone learns your password, she can t get into your account unless she has your phone, too) and restrictions by country. A good free version, and a decent deal at $12 a year for mobile access.

LastPass (shown) and other password managers can tell when you enter passwords into Web sites and will offer to remember them for you.

Dashlane: Probably the most beautiful of the password managers. David Pogue s choice (he also uses Apple s Keychain in parallel). Works across computers and mobile devices. Free on one computer, $29.99 a year for syncing across devices.

A good password manager, like Dashlane (shown) will look at all your passwords and tell you where you re reusing them a very unsafe practice!

Other password managers include KeePass, Roboform, Norton Identity Safe, DirectPass, Kaspersky Password Manager and SplashID. If you have one of these, great. Use it.

Step 2: Set it up with a really, really strong password.

Before you start putting passwords into your new password manager, configure it with a good, strong master password. In fact, don t think password, think passphrase. More than one word, a few symbols, all strung together in a unique order. yuMMy(Fuzzy)9&9baconbits something like that. You ll be typing it a lot, so give it a few tries with your fingers before committing (including on your mobile device s keyboard) to make sure it doesn t force any uncomfortable contortions.

Alternatively, you can come up with a shorter memorable passphrase that would never appear in a dictionary by using (for example), the first letters of the words in a sentence or title you won t forget. For example, IP17KBIMS! (I put 17 kidney beans in my salad!). However, even nonsense passwords can be hacked if they are short enough. Longer passwords are always better.

Either way, make sure you pick a passphrase you can remember. If you don t, you re cooked. A good password manager has no back door that will let you or the company who made it decrypt your data.

Step 3: Get it working on your computers and your mobile devices.

The idea of having a password manager is that it s one system that remembers your passwords across all your devices: computer, smartphone, tablet and so on. We recommend that you install it first on one computer, and in all the browsers you use, and set up the passphrase there, and then go to your mobile devices and other computers and repeat the process.

The software should walk you through the process of connecting all your devices to the same password manager account that stores all your passwords. Some systems, like LastPass, keep the passwords in their own system. Others, like 1Password, use somebody else s system, like iCloud or Dropbox.

Note that in every password manager worth anything at all, the password data you re storing is highly encrypted. It gets decrypted only on your devices. But you really want to have a good passphrase so your password file is protected when it s not on your computer.

Step 4: Start replacing your weak, repeating passwords with new ones.

Most good password managers will tell you where you are using duplicate passwords, which is your biggest vulnerability. Start with those. Look for high-value sites that are using passwords that you ve duplicated elsewhere, and change them first. Your password manager will be able to come up with strong passwords for you that don t even look like words. That s fine. You ll be using your password manager to enter your passwords into your accounts anyway.

Your most precious accounts are for banks and financial services, along with major sites that have financial data, like Amazon and Apple. Again, make sure you use different passwords for each account. That s more important than using strong passwords. But as long as you re using a password manager, make your passwords strong, too.

Then move on to gateway accounts like Facebook and Twitter, where a breach could have other ramifications, like identity theft.

You ll get tired of this job pretty quickly and probably won t finish at one sitting (or ever). That s why we recommend changing your most important accounts first, and especially that you decouple them from potential breaches at other sites by using unique passwords.

Step 5: Start using your password manager.

Try it out. Go to a site with a password you just created and, if you re logged in, log out. Then either go to the login page again or find the site through the search feature in your password manager. The manager plugin might spring into action and log you in itself, or you might have to press a button or a shortcut key to activate it. One thing you won t have to do is type in your password.

No password manager works perfectly on all sites, however, so you might have to copy and paste your password from the manager into your site or app. In most apps, there s a copy button that will do part of that job for you. If you have to type in your passwords by hand, then you re not using the manager to its fullest.

On iPhones and iPads, there is one wrinkle: A password manager can t enter passwords into apps or into browser fields (except Keychain when you re using Safari). You ll be using the copy-and-paste method on apps, and if you want your password manager to enter passwords automatically on mobile websites, then you ll have to use the manager s own app to find your site and then have it log you in on its own built-in browser. It s a drag to remember to do this, unfortunately.

But you are now more secure! Congratulations.

Step 6. Every now and then, change your password manager passphrase. Just in case.

Someone in Mexico Named a Child Facebook

Baby names have been getting progressively dumber in past years (maybe because we re now allowing Redditors to choose them). You can t swing a dead cat without hitting four Olyvyrs and a Daxxon at the local park.

So officials in one state Mexican state have taken matters into their own hands by banning the 61 names they ve deemed dumbest. Facebook is on the list and that means at least one kid in Sonora, Mexico, is named after the social network, because the names were culled from actual civil registries.

Other questionable names that were banned: Marciana, or Martian, and Circuncision, or Circumcision, The Associated Press reports. The state has also seen names like Juan Calzon, or Juan Panties, and a little girl named Lady Di.

The law is supposed to protect kids from being bullied, Sonora Civil Registry director Cristinia Ramirez has said, but who could ever even bother an 8-year-old named Lady Di?

Juan Panties, though, has a lot to live up to. Godspeed, little dude.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.